

@metpoliceuk how twitter is changing modern policing

Jamie Bartlett
Carl Miller

June 2013

@METPOLICEUK

**HOW TWITTER IS CHANGING MODERN
POLICING: THE CASE OF THE WOOLWICH
AFTERMATH**

Jamie Bartlett, Carl Miller

19 June 2013

Open Access. Some rights reserved.

As the publisher of this work, Demos wants to encourage the circulation of our work as widely as possible while retaining the copyright. We therefore have an open access policy which enables anyone to access our content online without charge.

Anyone can download, save, perform or distribute this work in any format, including translation, without written permission. This is subject to the terms of the Demos licence found at the back of this publication. Its main conditions are:

- Demos and the author(s) are credited
- This summary and the address www.demos.co.uk are displayed
- The text is not altered and is used in full
- The work is not resold
- A copy of the work or link to its use online is sent to Demos.

You are welcome to ask for permission to use this work for purposes other than those covered by the licence. Demos gratefully acknowledges the work of Creative Commons in inspiring our approach to copyright. To find out more go to www.creativecommons.org



Published by Demos 2013
© Demos. Some rights reserved.

Third Floor
Magdalen House
136 Tooley Street
London SE1 2TU

T 0845 458 5949
F 020 7367 4201

hello@demos.co.uk
www.demos.co.uk

INTRODUCTION

Major events – natural disasters, football matches, terrorist attacks – are increasingly accompanied by a complex, varied and evolving cloud of reaction on Twitter: questions, interpretations, condemnations, jokes, rumours and insults. This surge of online information, shadowing the event itself, is often called a ‘twitcident’.

This new kind of aftermath opens new opportunities and challenges for policing.ⁱ Inherently amenable to collection, measurement and analysis, they can be harnessed as sources of social media intelligence – ‘SOCMINT’ – in a number of ways to keep society safe: as important sources of evidence; as situational awareness in contexts that are changing rapidly, as a way of crowd-sourcing intelligence, and to answer a backdrop of strategic research questions, such as how society will change in result of the event itself.ⁱⁱ Twitcidents do not just provide intelligence for the police, however. They also put pressure on the police themselves to provide information, intelligence and, where possible, public assurances.

As we have argued elsewhere, social media is an increasingly important aspect of modern policing, particularly for intelligence collection and communication.ⁱⁱⁱ It is now apparent that social media is an important part of any large incident or emergency response. As people continue to transfer their social lives onto these digital-social spaces, the benefits of effectively harnessing and responding to twitcidents will increase, and so will the risk of failing to do so.

Woolwich

To understand the specific challenges and opportunities this presents, we have chosen to dissect in detail the tweets directed at @metpoliceuk immediately before, during and after the alleged murder of Lee Rigby by two individuals – believed to be Islamist extremists – in Woolwich at 14:20 on 22nd May 2013. After the murder, the alleged assailants remained at the scene, and spoke to, and were filmed by, bystanders. First unarmed, then armed police

arrived and, following an exchange of fire, the two men were wounded and taken to hospital.

As of May 29th the Metropolitan's Police Twitter account (@metpoliceuk) was the most followed police account in the UK, with 114,369 followers. Up to the afternoon of the 22nd, the account was lively. Two online petitions were driving tweets to the police account, one to demand additional information be released from the McCann investigation, and the other demanding the arrest of the self-exiled Pakistani politician Altaf Hussain.

BBC Breaking News' Twitter account tweeted at 3.50pm that:

Police officers called to incident in Woolwich, south-east London at 14:20 BST, @metpoliceuk confirm. No further details at present

Quickly, news of the attacks began to circulate on Twitter, and video footage of the assailants – including one of the suspects talking to a bystander – was uploaded onto YouTube and other platforms.

By the late afternoon, members of the English Defence League took to Twitter to organise a flash demonstration in Woolwich to express outrage at the murder; and by the early evening around 100 supporters clashed with police before being dispersed at around 11pm.

METHOD

In order to understand how people reacted on Twitter to these events, from May 17th to May 23rd, we 'scraped' all 19,344 Tweets that contained the identifying '@tag' - @metpoliceUK.

A Twitter scrape is the result of filtering the recent public Twitter timeline with a set of query terms through Twitter's 'Search Application Programming Interface'. All Tweets matching

@metpoliceuk were in this way accessed, and downloaded into a MySQL database.

With this corpus of collected tweets three simple analyses were conducted:

- Overall rates and volumes of tweets over time;
- A qualitative analysis of tweets to create overall ‘types’. Several thousand Tweets were manually placed into categories until ‘saturation’ – wherein new tweets neither required new categories to be created, or the boundaries of existing categories to be revised;
- The formal coding of 500 randomly selected tweets into these categories to establish the proportional breakdown of the dataset overall. This was done twice, the first, over the 24 hours of the 22nd, the second over the entire four days period during which the data was collected. This was in order to provide some broader analysis and comparison.

Ethics

In the UK, the standard best practice for research ethics is the Economic and Social Research Council (ESRC) ethical framework, which is made up of six principles.^{iv} Social media research of this kind is a new field, and the extent to which (and how) these ethical guidelines apply practically to research taking place on social media is unclear.

We believe that the most important principle to consider for this work is whether informed consent is necessary to re-use the Twitter data that we collected; and whether there is any possible harm to participants in re-publishing their Tweets that must be measured, managed, and minimised.

Informed consent is required where research subjects have an expectation of privacy. We believe that there is, in general, a low

level of privacy expectation to those who tweet publicly available messages. Twitter's Terms of Service^v and Privacy Policy^{vi} state: "What you say on Twitter may be viewed all around the world instantly. We encourage and permit broad re-use of Content. The Twitter API exists to enable this". We further determined that the 'reasonable expectation' of privacy of users was additionally unlikely given all users had 'broadcast' their tweet to a public and official account: @metpoliceuk.

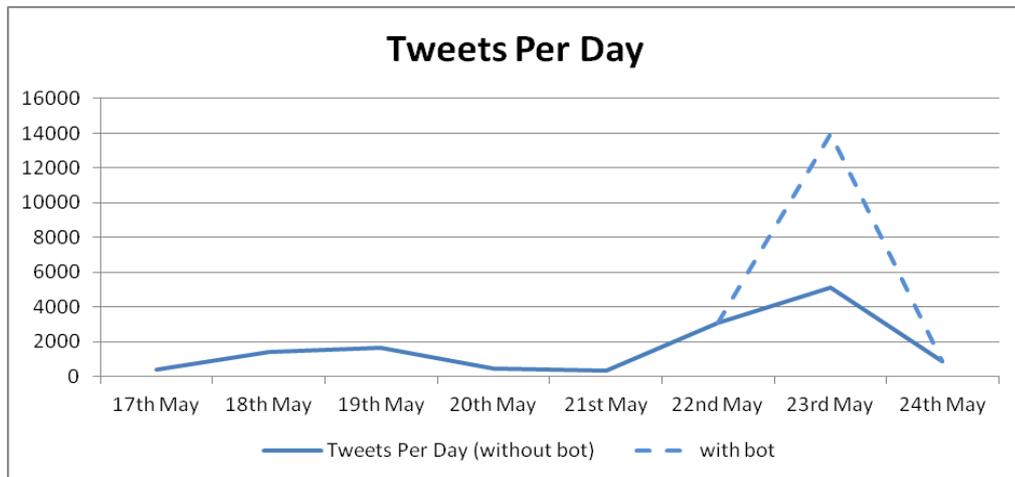
That does not remove the burden on researchers to make sure they are not causing any likely harm to users, given they have not given a clear, informed, express consent. Therefore, we carefully reviewed all tweets selected for quotation in this report and considered whether the publication of the tweet, and the links, pictures and quotations contained within, might result in any harm, distress, to the originator or other parties involved. For example, if any possibly invasive personal information were revealed in the body of the tweet, this was not used. As a further measure, we removed any user names; and in a small number of cases, 'cloaked' the text so it could not allow for the identification of the originator.

Results

Finding 1: Spike in activity.

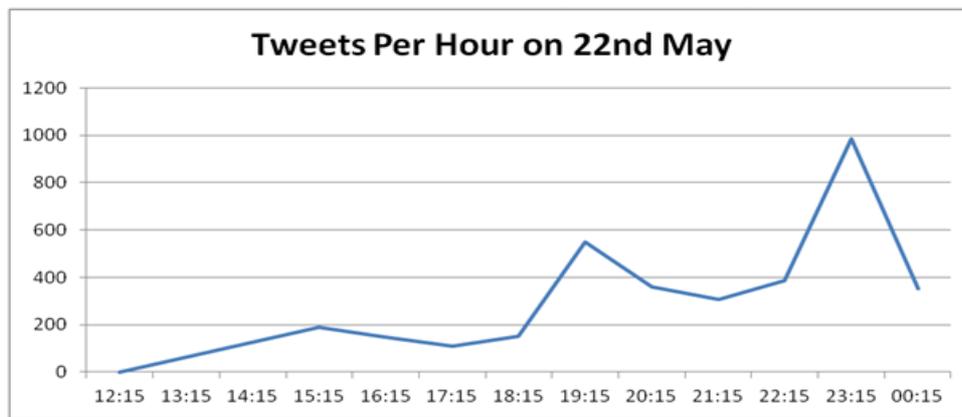
The first result is that (unsurprisingly) there was a large spike in activity on the day of the attack; and especially the day afterward, as details emerged.

@metpoliceuk tweets 17 – 24 May



(dotted line inclusive of bot tweets)

@metpoliceuk tweets on the 22nd May (inclusive of bot tweets)



Significant is the sheer volume. Tweets arrived at such a speed on the day of the 22nd as to make it extremely difficult to effectively deal with. On the 22nd itself, the account received around 14,000 messages, of which the majority – around 9,000 – were bot generated. Bots are fake accounts that often try to – in their name, profile, tweets and behaviour – appear human. These fake accounts often, as was the case here, participate in a network – or ‘bot net’. This network can be controlled by a single, ‘master’ account, or at number of different points. Botnets are diverse and, operating for a number of reasons (or no apparent reason at all),

they are only united in their tactic of utilizing inauthentic accounts to manipulate the propagation of a message.

Reaction to Woolwich did not occur in isolation, however. On the 17th and 18th of May, thousands of tweets flooded into the Met account calling for the arrest of Altaf Hussain, the leader of the Pakistan political party Muttahida Qaumi Movement.^{vii} Events in the evening saw the greatest volume of activity, which was both in respect of further details emerging, and the English Defence League’s decision to demonstrate in Woolwich that evening.

Finding 2: wide variety of use-types (after the removal of bot-generated tweets)

	19-23rd	22nd
Petition	23.2 %	4%
Reporting a possible crime on social media (ie death threats)	20.6 %	20.3%
Indirect mention	19.4 %	34.4%
Irrelevance / incomprehensible	13.6 %	3.4%
Conversational	11 %	15.5%
Re-tweeting	6 %	13%
Sending offline evidence	2.4 %	2%
Rumour / trolling	1.6 %	4.6%

Gaming / bots	1.4 %	0.0%
Sousveillance (ie reporting on police activity)	0.8%	2.8%

The second significant finding was that the twitcident was extremely diverse: it contained, in our estimation, ten different types of interaction of vastly differing scales of usefulness. The proportional breakdown of these different kinds of Tweets changed significantly over time.

Different types of tweets received by the @metpoliceuk account

Looking in further detail at each of the use-types that flooded into @metpoliceuk and on the 22nd paints a clearer picture of the opportunities and difficulties that they offer and pose.

Gaming/bots

Roughly half of the tweets encountered were judged to be fake, sent from non-human, automated 'bot' accounts. 8,816 (45 per cent) of the original sample of 19,344 tweets were produced by a single bot network propagating the following message:

*Half the things people are tweeting should put them in jail @metpoliceuk
The news hasnt even got confirmed stories yet! #Woolwich #Racism*

The originating account of this tweet was found. It is not apparent that it either solicited the large number of retweets it received, has had any other tweet retweeted at such volume, or in fact willingly participated in the botnet at all. The attributes and behaviour of the account suggest it is an authentic one.

The inauthentic ‘bot’ accounts have subsequently been deleted. They were however markedly different. They produced no original tweets themselves had no followers, participated in no conversations, and retweeted in unison. The messages this particular network did propagate gave no clue as to the underlying purpose of the network – many tweets were incomprehensible, and, collectively, did not indicate either clear intent, bias or motivation.

Sending offline evidence (2.4% / 2%)

A small number of the most potentially useful tweets were those that referred evidence to the police that the Tweeter seemed to genuinely consider to be legally relevant. This included cases of eyewitness accounts of crimes they had witnessed or were aware of:

‘@metpoliceuk yesterday in coach leaving from London Victoria at 10pm to Birmingham a person was openly racist towards another individual.’

‘@xxx @metpoliceuk Hotel xxx, xxx told us to shut our dog in our car on a hot day! We checked out instead! Dog owners be warned.’

In several cases this included alerting the authorities to what was taking place as events unfolded:

‘@xxx: Reports of two busloads of #EDL are on their way to #Woolwich via @xxx cc @UK_Collapse"@metpoliceuk’

In some instances these also included information that might be extending beyond the police, and drawing attention of a wider population:

‘@Broadway_Mkt @E9_Resident @metpoliceuk @hackneygazette WARNING: bag thieves London Fields. 2 men, white plastic bag. Stolen black handbag’

Even though the Metropolitan Police has repeatedly asked that emergency calls should not be directed through Twitter, there were some examples where, if true, 999 may have been more appropriate:

'@metpoliceuk #Stalkers with #listening devices threatening #Jamaican lady near Meadowbrook High Sch St Andrew #Jamaica 11:48am 23.5.2013'

Reporting a possible crime on social media (20.6 % / 20.3%)

More common was the referral of social media content itself as evidence about alleged or supposed online and offline crimes. Very often they came attached with an investigation, typically in the form of a Twitpic or other photographic 'evidence'.

'@metpoliceuk stop these people <http://t.co/xxx>

The most common kinds of complaint/referral made to the police fell into a broad family of complaints about the content of other social media messages or tweets, alleging instances of threats, bullying, and racism. Examples include:

'@xxx: @xxx answer or ill slit your throat. ?" @metpoliceuk'

@metpoliceuk please do something about this anti Semitic abuse I just received. <http://t.co/xxx>

'@metpoliceuk hello I am being cyber bullied by twitter user xxx please help me

*'@xxx: Why don't all the english get together and kill the muslims! "
@metpoliceuk please report this lady for incitement to murder*

As the nature of the Woolwich killing became clear, material was passed on to the police with an apparently preventive aspiration of demonstrating Islamophobic plots and incipient violence:

'English Defence League's xxx aka xxx threatens bombmassacre of Muslims <http://t.co/xxx> #edl #woolwich @metpoliceuk #croydon

Alongside tweets objecting to the content of other tweets, tweets were identified alleging driving infractions, fraud, involvement in riots, paedophilia, child abuse, drug-taking, cyber-bullying and animal abuse. They usually include the Tweeter pleading with the police to investigate the case under question:

"@xxx: I was driving with no Insurance and a provisional before i passed and never got caught ??stupid but #thuglife"<< @metpoliceuk

"@xxx: To me, attending London riots was like a big rave except you walk out at the end with a party bag loool" | @metpoliceuk ^_^

"@xxx: <http://t.co/xxx>" @NSPCC @CHILDLINE1098 @metpoliceuk ???

"@xxx: @xxx_ @xxx I slap my dad all the time he just hits me back twice as hard lmao" @metpoliceuk @childline

@metpoliceuk this is illegal. RT@xxx: @xxx YESSS, I AM FINE I JUST TOOK SOME DRUGS THAT CAN HELP ME, YOU GET ME

@xxx @xxx Kate&Gerry #McCann fooling the public,the people who donate to their fund @metpoliceuk please investigate THAT FUND

@metpoliceuk "wenger has fucked another young black French boy" this vile and libellous tweet by #arsenal "fan" @xxx

These referrals also spanned evidence on other Internet platforms:

On @LinkedIn and in 'British Mensa Limited - Business network' debate on how to murder someone by hiring a contract assassin.

@SonOfTheWinds @Cyclestrian @metpoliceuk @MayorofLondon you can have a look at the website <http://t.co/1zO6zryQY0>

Indirect mention of the police (19.4 % / 34.4%)

A still larger proportion of tweets used the @metpoliceuk handle indirectly, as a way of identifying the police, but not apparently requiring or demanding an answer from them. People did this for a wide array of purposes, including comments on performance – both criticism and (more commonly) support:

Called @metpoliceuk over an hour ago to report 2 pissed fellas using the square park as a toilet, bin and bed - no sign of 'em typical

Deaths in custody of young black men and those with mental health issues still a stain on @metpoliceuk #bbcsp

My thoughts are with all the staff from @metpoliceuk tonight stay safe out there #donriotplaceapoppyinstead #holdtheline

Well done to the Woman Police Officer from @metpoliceuk for not shooting yesterday's suspects dead. Hopefully they'll live to face justice

Conversational/engagement (11% / 15.5%)

@metpoliceuk also receive a significant number of direct requests for information or a response. This included for simple information:

@metpoliceuk Hi who do i contact about a recent fire?

People resorting to Twitter due to other failed attempts to reach the police:

@metpoliceuk every number i've been given to call you back regarding a crime, either "Unavailable" or Rings Out! Please Help! #Frustrating

Challenges to the police for more information:

Think @metpoliceuk need to speak. It's not about scuppering an inquiry. It's about quelling rumour now. And MSM need to catch up & demand it

And for reassurance following Woolwich itself:

@metpoliceuk are there still suspects on the loose in Woolwich?

Petition (23.2% / 4%)

In addition to individual cases of conversation and engagement with the police, there was also strong evidence of systematic cooperation by large bodies of people to concertedly appeal and petition the police on Twitter to influence their policy. There were two petitions in evidence. First, a systematic campaign calling for the arrest of Altaf Hussin, the leader of the Pakistan political party Muttahida Quami Movement, where he is alleged to have responded to accusations of electoral fraud with threats of violence, then actually carried out in Karachi. The MET launched an investigation “following complaints”.^{viii} The second was a campaign for the police to release more information on their investigation into the disappearance of Madeleine McCann.

Twitter itself was used to help coordinate this kind of concerted and collective messaging:

pls tag @metpoliceuk in the tweets against killing of Zehra Hussain and against Altaf Hussain

Retweeting(6% / 13%)

There was a significant amount of straightforward retweeting of official police tweets, sometimes with an attached commentary of gloss, often supportive.

Obvious rumour/trolling (1.6% / 4.6%)

Trolling refers to the practice of spreading intentional misinformation or abuse usually in order to provoke a response. However, the small proportion of tweets coded as such in this analysis reflects the difficulty of immediately assessing a Tweet as obviously incorrect, rather than the absence of incorrect Tweets within the sample. Some users appears to be trying to link the Woolwich killing, in the immediate aftermath, to the Pakistani group PTI:

There are NO Good Taliban They All Are Bad & London Incident Is Occurred Today Shame #PTIBehindLondonAttack @David_Brown @MetPoliceUK'

Sousveillance (0.8% / 2.8%)

Police activity is often watched and shared via Twitter; something academics have termed 'sousveillance': the recording of actions of the police by members of the public, either text or picture taken from their phone. This is sometimes a general claim or comment of a very specific example (often related to driving):

7 police riot vans heading west on Park Royal section of A40. Looks like something's kicking off somewhere. Anyone know what? @metpoliceuk

@BBCNews Why @metpoliceuk can unmarked police car BX59BYM choose 2 go through a red light on hanger lane wiv no blues & 2's on? #1rule4us

@metpoliceuk police once again taking liberties or are they allowed in bus lanes . No siren <http://t.co/9bDUYsqxwz>

CONCLUSION

In the immediate aftermath of Woolwich, there was a huge surge in different types of interaction with the police. This is something all police forces now have to contend with. As this short analysis shows, the spikes in volume are a mixed blessing: they include both potentially useful information, but also a lot of hearsay, rumour and unreliable information.

Opportunities

A kernel of possibly the most useful tweets contain evidence of alleged crimes, both online and offline. This includes eyewitness testimony, prompts of investigations, pictorial evidence of allegedly hateful speech, and direct (sometimes quite desperate) requests to the police for help or protection. A large proportion are based on material drawn from social media, and specific to social media: online objectionable speech and cyber-bullying.

In addition to provision of evidence, the analysed tweets can provide intelligence and insight: 'SOCMINT'. Taken individually, tweets contained eye-witness reportage, possible tip-offs, and – in mentions of the police - information on how the police in general, or their specific actions, were viewed and received by members of the public. The tweets can also be subject to aggregate analysis to more strategically measure groundswells of emotion – such as violence or heat – occurring after a major event.

One of the key strengths of Twitter is its ability to establish reciprocal individual-level interactions rather than mass broadcasts. Many tweets were overtures to the police for just this kind of interaction. In the uncertain and challenging aftermath of a major event, a police response to these overtures can be extremely valuable: rebutting rumours, providing assurance to the public and producing information and advice to help people keep themselves, and society, safe.

However, this also points to a number of new pressures and challenges for the police.

Challenges

Especially during fast moving events, responses by the police must be rapid and agile. The first and most readily obvious challenge is the sheer scale and variety of tweets that are generated following major incidents. Whilst other fields have developed automated procedures to handle the scale of information produced on social media, these technologies are not yet able analyse information the precision and accuracy required to respond to, and intervene within possibly serious situations. Any manual analysis of tweets would struggle to cope with such scales to produce analysis or allow action within the tight, pressured timescales required in the context of rapidly evolving events.

Whether challenged on a policy, sought-after for information, or contacted to investigate an alleged crime, there was a strong expectation and requirement in many of these tweets for the police to respond. It became clear that a non-response from the police, in many different contexts, could lead to a negative outcome: an emboldened rumour, an infuriated questioner, or a neglected victim. It appears to us that the Met account has allowed many more people to engage with the police, and that many look to the feed as an important source of information. Maintaining this integrity and trust is clearly vital.

However, these incidents are especially difficult to understand and act upon. Trustworthy citizen-journalism, pressing demands and revealing insights sit side-by-side with lazy half-truths, deliberate mistruths, ironies, trolling and general nonsense. Sorting through this mass of information, especially at the speed demanded by the tempo of the twitcident itself, is a formidable intellectual, technological and operational challenge.

As with any intelligence, SOCMINT should improve decision-making by reducing ignorance.^{ix} However, verifying and corroborating Tweets are very difficult. People share stories on Twitter for lots of reasons, and not always because they think it is accurate. Outlandish rumours often spread quickly, because they are interesting, and people like interesting things. During the

London riots, stories of tigers loose on Primrose Hill and the Army at Bank went viral, and this weight gave them a credibility it took hours to crack. This is made harder because context is often lost such as motives and reliability of the source or why it was said. Sometimes there may even be intentional misinformation: already there is a considerable amount of non-authentic and fake accounts (sometimes called ‘sock puppets’) on many social media platforms. Facebook recently revealed that seven per cent of its overall users are fakes and dupes.^x Sometimes that might even be people that have motive to intentionally mislead the authorities for a variety of purposes.

Underlying this, there are legal and ethical questions – still open – as to how the police can collect and use social media information in a way that is proportionate, legal and can command public confidence and support. The official collection and use of social media information is a controversial and contested practice, especially for the purposes of intelligence and security.

RECOMMENDATIONS

It is vital that the police respond to maximise the benefits of this new information landscape. This paper suggests three changes that might be considered to help with that task.

Recommendation 1: Each constabulary should have the human and technological infrastructure to deal with social media aftermaths in emergency scenarios.

Social media serves as a valuable type of two-way communication between the police and the public; but in times of emergencies, it can also become an incredibly important source of real time insight. This means that constabularies need to have a capability flexible enough to respond to these different demands. This would include:

- A single dedicated, operational lead for social media
- A single point of contact to manage and filter social media requests and conversations, which includes 24 hour staffing of those accounts (either central or local) judged likely to be the most important channels of information exchange during a twitcident
- Development of a triage capability to quickly filter different types of information: a procedure to determine which demands need to be followed-up, acted on, investigated further, and which can be dismissed. This capability would consist of a series of automated and manual procedures
- Integrating social media monitoring into control centres
- Managing possible jurisdictional issues, such as who takes responsibility for investigations where there is a lack of clarity over location of offence
- Taking responsibility for the correct use of social media accounts, managing engagement, crowd-source intelligence collection (such as #shopalooter), reviewing existing capability, or neighbourhood engagement (such as e-neighbourhood watch). A decision needs to be taken with respect to whether and how Twitter accounts should respond to certain rumours and discussions.
- Managing the public's expectations about what can and cannot be done in terms of 'social media policing' such as troll investigations, cyberbullying and low-level identity theft.

Recommendation 2: A centralised SOCMINT 'hub' should be created.

Alongside specific force level capabilities, the Police need to evolve and strengthen strategic SOCMINT capabilities more generally across the country. A single, networked hub of excellence and

managed network of experts should coordinate SOCMINT development across different branches of the police. Structures of engagement and funding must be created to involve extra-governmental, especially industrial and academic actors where possible. This hub should:

- Collect, store and analyse social media feeds, and develop methods for use by forces. In particular these should include new ways to triage and filter large volumes of data to allow for more rapid processing
- Manage relationships with the major platform providers in a strategic way: including reporting breaches of terms and conditions rather than taking a legal route
- Produce specialised training for intelligence analysts and those who will work closely with the Crown Prosecution Service. This includes the possible risks of social media use: such as the identification of personal information relating to individuals officers.
- Advise on purchasing and commissioning decisions, so individual constabularies do not purchase or lease ineffective, over-priced technologies that do not deliver any value or benefit
- Review the code and guidance for the management of police information for dealing with very large volumes of personal data
- Evaluate the effectiveness of methods and techniques applied across the forces

Recommendation 3: The Home Office should create a clear legal framework for the collection and use of SOCMINT.

The police will sometimes need to access social media for intelligence work, in a variety of intrusive and non-intrusive ways. But as it stands, the legal basis for SOCMINT is not clear, nor

necessarily publicly understood or accepted. While tweets directed at the Met are clearly open source and would not require any authorisation to collect, it is important that the sort of capabilities that might be built to help that process is also regulated and limited. The collection and use of intelligence from social media must be placed on a firm regulatory basis that is publicly argued and commands public confidence. As we have argued elsewhere, different types of collection and use of SOCMINT can fit under the existing categories under the current Regulation of Investigatory Power Act (RIPA):

- *Covert directed surveillance* When private information about a person is taken from a public domain where there is a reasonable expectation of privacy, authorisation should be required under RIPA under existing measures that cover Directed Surveillance and Covert Human Intelligence.
- *Covert human intelligence sources* If the police establishes or maintains a personal or other relationship with a person for the covert purpose of obtaining information about them, or to get access to information about another individual using social media, it should be classed as a covert human intelligence source. Authorisation should be required under RIPA under existing measures that cover Directed Surveillance and Covert Human Intelligence.
- *Intercept* Intelligence gathered from social media that makes available the content of a communication, while it is being transmitted, to a person other than the sender or intended recipient, by monitoring, modifying or interfering with the system of transmission should fall under Chapter I of Part I of RIPA. This requires a warrant from the Home Secretary.

Inevitably, as the way we communicate changes, so must the ways in which we maintain law and order. However, digital freedom and liberty are increasingly important for citizens, and some aspects of policing work are not amenable to the norms and mores of social media. We therefore recommend that the police proceed with care.

They should not underestimate the potentially transformative power of social media to their work, nor underestimate the legitimate concerns citizens have about misuse. The use of social media should be guided by the same principles that underpin all police activity - public confidence and legitimacy, accountability, visible compliance with the rule of law, proportionality, the minimal the use of force, and engagement with the public.

Demos – Licence to Publish

The work (as defined below) is provided under the terms of this licence ('licence'). The work is protected by copyright and/or other applicable law. Any use of the work other than as authorized under this licence is prohibited. By exercising any rights to the work provided here, you accept and agree to be bound by the terms of this licence. Demos grants you the rights contained here in consideration of your acceptance of such terms and conditions.

1 Definitions

a 'Collective Work' means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this Licence.

b 'Derivative Work' means a work based upon the Work or upon the Work and other pre-existing works, such as a musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work or a translation from English into another language will not be considered a Derivative Work for the purpose of this Licence.

c 'Licensor' means the individual or entity that offers the Work under the terms of this Licence.

d 'Original Author' means the individual or entity who created the Work.

e 'Work' means the copyrightable work of authorship offered under the terms of this Licence.

f 'You' means an individual or entity exercising rights under this Licence who has not previously violated the terms of this Licence with respect to the Work, or who has received express permission from Demos to exercise rights under this Licence despite a previous violation.

2 Fair Use Rights

Nothing in this licence is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3 Licence Grant

Subject to the terms and conditions of this Licence, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) licence to exercise the rights in the Work as stated below:

a to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;

b to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works; The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. All rights not expressly granted by Licensor are hereby reserved.

4 Restrictions

The licence granted in Section 3 above is expressly made subject to and limited by the following restrictions:

a You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this Licence, and You must include a copy of, or the Uniform Resource Identifier for, this Licence with every copy or phonorecord of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this Licence or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this Licence and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this Licence Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this Licence. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any reference to such Licensor or the Original Author, as requested.

b You may not exercise any of the rights granted to You in Section 3 above in any manner that is primarily intended for or directed toward commercial advantage or private monetary compensation. The exchange of the Work for other copyrighted works by means of digital filesharing or otherwise shall not be considered to be intended for or directed toward commercial advantage or private monetary compensation, provided there is no payment of any monetary compensation in connection with the exchange of copyrighted works.

C If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Collective Works, You must keep intact all copyright notices for the Work and give the Original Author credit reasonable to the medium or means You are utilizing by conveying the name (or pseudonym if applicable) of the Original Author if supplied; the title of the Work if supplied. Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5 Representations, Warranties and Disclaimer

A By offering the Work for public release under this Licence, Licensor represents and warrants that, to the best of Licensor's knowledge after reasonable inquiry:

i Licensor has secured all rights in the Work necessary to grant the licence rights hereunder and to permit the lawful exercise of the rights granted hereunder without You having any obligation to pay any royalties, compulsory licence fees, residuals or any other payments;

ii The Work does not infringe the copyright, trademark, publicity rights, common law rights or any other right of any third party or constitute defamation, invasion of privacy or other tortious injury to any third party.

B except as expressly stated in this licence or otherwise agreed in writing or required by applicable law, the work is licenced on an 'as is' basis, without warranties of any kind, either express or implied including, without limitation, any warranties regarding the contents or accuracy of the work.

6 Limitation on Liability

Except to the extent required by applicable law, and except for damages arising from liability to a third party resulting from breach of the warranties in section 5, in no event will licensor be liable to you on any legal theory for any special, incidental, consequential, punitive or exemplary damages arising out of this licence or the use of the work, even if licensor has been advised of the possibility of such damages.

7 Termination

A This Licence and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this Licence. Individuals or entities who have received Collective Works from You under this Licence, however, will not have their licences terminated provided such individuals or entities remain in full compliance with those licences. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this Licence.

B Subject to the above terms and conditions, the licence granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different licence terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this Licence (or any other licence that has been, or is required to be, granted under the terms of this Licence), and this Licence will continue in full force and effect unless terminated as stated above.

8 Miscellaneous

A Each time You distribute or publicly digitally perform the Work or a Collective Work, Demos offers to the recipient a licence to the Work on the same terms and conditions as the licence granted to You under this Licence.

B If any provision of this Licence is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Licence, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

C No term or provision of this Licence shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

D This Licence constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This Licence may not be modified without the mutual written agreement of Demos and You.

NOTES

ⁱ There are a number of possible ways to classify police social media use. The COMPOSITE project, funded under the EU's FP7 programme identifies nine: Social Media as a Source of Criminal Information; Having a Voice in Social Media; Social Media to Push Information; Social Media to Leverage the Wisdom of the Crowd; Social Media to Interact with the Public; Social Media for Community Policing; Social Media to Show the Human Side of Policing; Social Media to Support Police IT Infrastructure; Social Media for Efficient Policing. Deneff et al, *Best Practice in Police Social Media Adaptation*, 2010, <http://www.fit.fraunhofer.de/content/dam/fit/de/documents/COMPOSITE-social-media-best-practice.pdf> (accessed 28 Feb 2013)

ⁱⁱ Omand, D., Bartlett, J & Miller, C (2012) *#Intelligence*; Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data*, John Murray, London: 2013

ⁱⁱⁱ Bartlett, J, Crump, J, Miller, C & Middleton, L (2013) *Policing in an information age*, Demos

^{iv} The six principles are: 1) research should be designed, reviewed and undertaken to ensure integrity, quality and transparency; 2) research staff and participants must normally be informed fully about the purpose, methods and intended possible uses of the research, what their participation in the research entails and what risks, if any, are involved; 3) the confidentiality of information supplied by research participants and the anonymity of respondents must be respected; 4) research participants must take part voluntarily, free from any coercion; 5) harm to research participants and researchers must be avoided in all instances; 6) the independence of research must be clear, and any conflicts of interest or partiality must be explicit. ESRC, Framework for Research Ethics, latest version: September 2012, http://www.esrc.ac.uk/_images/Framework-for-Research-Ethics_tcm8-4586.pdf (last accessed 27.03.2013)

^v Twitter Terms of Service, <http://www.twitter.com/tos> (Accessed 27.03.2013)

^{vi} Twitter Privacy Policy, <http://www.twitter.com/privacy> (Accessed 27.03.2013)

^{vii} <http://www.bbc.co.uk/news/world-asia-22559282>

^{viii} <http://www.bbc.co.uk/news/world-asia-22559282>

^{ix} As defined by David Omand in *Securing the State*.

^x Eaton, E. (2012). There are more 'Fake' People on Facebook than Real Ones on Instagram. *Fast Company*

Twitter has transformed people's response to crimes and how they engage with authorities like the police. Never was the changing nature of communication clearer than after the vicious attack on Drummer Lee Rigby in Woolwich. Twitter became a first port of call for many eye witnesses, while the perpetrators actively goaded onlookers into sharing evidence of their criminal acts on the internet.

The @MetPoliceUK paper compiles almost 20,000 tweets that included the tag @MetPoliceUK from the week of the Woolwich attack. In-depth analysis breaks down what information people were sharing online, when they shared it and its value as a source of information. It finds that while there is plenty of spam and other useless information swirling around the social network, many people do use it to provide useful information, such as reporting a crime or sending evidence.

The paper argues that this new medium creates opportunities and challenges for policing. It recommends that authorities should harness the power of social media intelligence - or SOCMINT - through establishing a centralised hub and specialists in each constabulary, to ensure they are able to interpret and respond to messages received. This would provide another tool in their vital job of reassuring the public and helping to keep them safe.

Jamie Bartlett is Director of the Centre for the Analysis of Social Media (CASM) at Demos. Carl Miller is Research Director at CASM.